doi：10. 12068/j. issn. 1005－3026. 2026. 20269030

一种基于简单模型的n维离散无简并超混沌系统构建方法

范春雷，方冬华，丁 群
（黑龙江大学 电子工程学院，黑龙江 哈尔滨 150080）

摘 要：为解决数字混沌在有限域中的动力学退化问题，本文提出了1种简单的数学模型，用于生成具有任意指定数量正Lyapunov指数（LE）的n维离散无简并超混沌系统．本文揭示了雅可比矩阵的奇异值与系统Lyapunov指数之间的内在联系．基于拉伸与折叠的思想，所提模型采用幂函数和指数函数以获取足够大的Lyapunov指数，同时采用常规三角函数确保系统的有界性．为验证所提方法的有效性与灵活性，本文给出了理论证明及2个系统构建示例．最后，基于此设计了1个具有良好统计特性的混沌伪随机数生成器．所提的无简并超混沌系统模型结构简单、动力学特性强，非常适用于信息安全与保密通信领域．

关 键 词：无简并混沌；动力学退化；伪随机序列；奇异值分解（SVD）；Lyapunov指数
中图分类号：O 415.5 **文献标志码**：A **文章编号**：1005-3026（2026）07-0099-08

A Construction Method for n-Dimensional Discrete Non-degenerate Hyperchaotic Systems Based on a Simple Model

FAN Chun-lei, *FANG Dong-hua*, *DING Qun*
（School of Electronic Engineering, Heilongjiang University, Harbin 150080, China. Corresponding author: FAN Chun-lei, E-mail: 2020021@hlju.edu.cn）

Abstract: To address the issue of dynamical degradation of digital chaos in finite fields, this paper proposes a simple mathematical model for generating n-dimensional discrete non-degenerate hyperchaotic systems with an arbitrary number of specified positive Lyapunov exponents (LEs). This paper reveals the intrinsic relationship between the singular values of the Jacobian matrix and the LEs of the system. Based on the idea of stretching and folding, the proposed model uses power and exponential functions to obtain sufficiently large LEs, while using conventional trigonometric functions to ensure system boundedness. To verify the effectiveness and flexibility of the proposed method, theoretical proofs and two system construction examples are provided. Finally, based on this, a chaotic pseudo-random number generator with good statistical properties is designed. The proposed non-degenerate hyperchaotic system features a simple structure and robust dynamical characteristics, making it highly suitable for applications in information security and secure communication.

Key words: non-degenerate chaos; dynamical degradation; pseudo-random sequence; singular value decomposition (SVD); Lyapunov exponent

混沌理论表明，看似无序的系统中往往隐藏着有序的结构与规律．混沌系统具有诸多优良特性，如内在随机性、有界性、对初始条件的敏感性以及遍历性等，这些特性与密码学中混淆和扩散两大基本原则天然契合．因此，混沌理论在信息安全与保密通信领域得到了广泛应用，例如混沌伪随机数生成器[1-2]、基于混沌的信息隐写术[3]、基于混沌同步的保密系统[4]以及混沌密码学[5]等．

收稿日期：2026-04-05
基金项目：国家自然科学基金资助项目（62101178）；黑龙江省省属本科高校“优秀青年教师基础研究支持计划”资助项目（YQJH2025191）．
作者简介：范春雷（1991—），男，黑龙江哈尔滨人，黑龙江大学教授．
通信作者：范春雷，E-mail：2020021@hlju.edu.cn.

然而,由于计算机与微处理器有限计算精度的不利影响,数字化混沌系统的动力学特性会不可避免地发生退化,这种退化现象严重制约了混沌在工程实践中的应用.为应对有限域内数字混沌的动力学退化问题,研究者已提出多种抗退化方案,包括混沌轨道随机跳转方法[6]、利用有限精度误差方法[7]、扰动法[8]、位循环移位法[9]和模数混合法[10]等.这些方法大多旨在增强低维数字化混沌映射的动力学特性,但增强后的低维混沌映射在循环长度、序列复杂度和随机性等方面相较某些高维超混沌系统优势并不明显.在高维超混沌系统的构建方面,早期设计策略主要依赖状态反馈控制、耦合非线性项以及参数试错等方法[11-12].这些方法缺乏充分的理论支持,仅凭经验与技巧难以设计出理想的高维超混沌系统[13].2017年,He等[14]提出了平均特征值准则,用于构建具有最多正Lyapunov指数数量的连续时间无简并超混沌系统.随后,Huang等[15]提出了1种具有周期性忆阻函数和复杂动力学行为的n维无简并超混沌系统.2018年,Wang等[16]创新性地提出通过预设常系数矩阵元素来构建具有n个正Lyapunov指数的n维无简并离散混沌模型的方法.此后,类似方法被进一步应用于构建基于常系数矩阵与模运算的离散无简并超混沌系统中[17-19].2023年,Fan等[20]提出了构建具有任意所需正Lyapunov指数数量的多项式超混沌通用模型及其几何控制方法.

基于上述分析,现有的高维无简并超混沌系统多依赖于稠密常系数矩阵与模运算.随着系统维度的增加,此类系统的计算复杂度呈$O(n^2)$级数增长.相比之下,本模型构建了1种以三角函数为折叠机制、以指数/幂函数为拉伸机制的环形耦合结构.模型没有使用硬性的边界截断,而是使用sin和cos函数作为天然的有界折叠机制.这种几何上的平滑折叠保留了非线性系统的复杂拓扑性质.此外,这种无常系数矩阵的设计将单步迭代的计算复杂度降低至$O(n)$,显著提升了系统向超高维扩展时的运算效率.在空间复杂度方面,本模型摒弃了传统高维混沌系统中矩阵存储所需的$O(n^2)$空间开销,仅需$O(n)$的线性存储空间,从而大幅降低了在嵌入式系统中的内存占用与片上资源消耗.值得注意的是,尽管底层的非线性函数(三角函数、幂函数等)单次运算开销高于常数乘法,但在配备硬件浮点运算单元(floating point unit, FPU)和优化数学库的现代数字信号处理器(digital signal processor,DSP)上可被高效地执行.最重要的是,本系统以$O(n)$线性增长的计算开销,换取了极大的正Lyapunov指数,而更大的Lyapunov指数意味着系统对初始条件更为敏感.所提模型利用幂函数与指数函数实现相邻轨迹的快速分离,控制参数的变化可显著调节n维离散超混沌系统的局部熵值.相关的随机性测试与混沌系统DSP硬件实现结果表明,该混沌模型具有良好的工程应用前景.

1 无简并超混沌系统构建理论与方法

1.1 基于SVD的Lyapunov指数计算法

奇异值分解(SVD)是线性代数中1种精妙而强大的工具,能够揭示矩阵最本质的变换.这一重要的矩阵分解方法在数值计算、图像与信号处理、机器学习、数据压缩等众多领域具有广泛应用.1个$m\times n$的矩阵$\boldsymbol{A}$的SVD能被定义为

$$\boldsymbol{A}=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}}. \tag{1}$$

其中:$\boldsymbol{U}$和$\boldsymbol{V}$分别为$m\times m$和$n\times n$的正交矩阵;$\boldsymbol{\Sigma}$为$m\times n$的矩形对角矩阵,其对角线上的元素为非负实数;T为矩阵转置运算.进一步,$\boldsymbol{\Sigma}=\mathrm{diag}(\sigma_1,\sigma_2,\cdots,\sigma_p)$且$\sigma_1\geqslant\sigma_2\geqslant\cdots\geqslant\sigma_p\geqslant0$,其中$\sigma_i(i\in\{1,2,\cdots,p\})$表示第$i$个奇异值,$p=\min(m,n)$.奇异值分解中矩阵乘法的可视化图如图1所示.

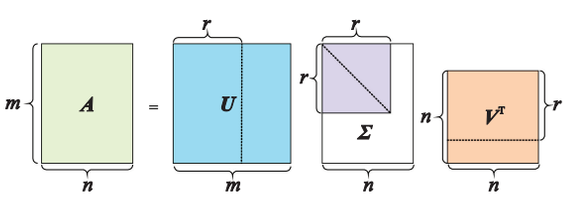


图1 奇异值分解中矩阵乘法的可视化图

Fig. 1 Visualization of the matrix multiplications in SVD

图中r表示矩阵$\boldsymbol{A}$的秩.基于图1,SVD可进一步表示为

$$\boldsymbol{A}=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}}=\begin{bmatrix}\boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_m\end{bmatrix}\begin{bmatrix}\sigma_1 & & & & \\ & \sigma_2 & & & \\ & & \ddots & & \\ & & & \sigma_r & \\ & & & & \ddots\end{bmatrix}\cdot$$

$$\begin{bmatrix}\boldsymbol{v}_1^{\mathrm{T}}\\ \boldsymbol{v}_2^{\mathrm{T}}\\ \vdots\\ \boldsymbol{v}_n^{\mathrm{T}}\end{bmatrix}=\begin{bmatrix}\sigma_1\boldsymbol{u}_1 & \sigma_2\boldsymbol{u}_2 & \cdots & \sigma_r\boldsymbol{u}_r & 0 & \cdots & 0\end{bmatrix}\begin{bmatrix}\boldsymbol{v}_1^{\mathrm{T}}\\ \boldsymbol{v}_2^{\mathrm{T}}\\ \vdots\\ \boldsymbol{v}_n^{\mathrm{T}}\end{bmatrix}=$$

$$\sigma_1\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}+\sigma_2\boldsymbol{u}_2\boldsymbol{v}_2^{\mathrm{T}}+\cdots+\sigma_r\boldsymbol{u}_r\boldsymbol{v}_r^{\mathrm{T}}=\sum_{i=1}^{r}\sigma_i\boldsymbol{u}_i\boldsymbol{v}_i^{\mathrm{T}}. \tag{2}$$

式中,$\boldsymbol{u}_i$ 和 $\boldsymbol{v}_i$ 分别为对应的左奇异向量和右奇异向量,左、右奇异向量通过奇异值 σ_i 成对关联,共同实现了矩阵 $\boldsymbol{A}$ 从右空间到左空间的线性映射.进一步,基于 SVD 计算 Lyapunov 指数的详细步骤如下.

步骤 1　假设 $\boldsymbol{U}_0$ 是 $n\times n$ 的正交矩阵,例如单位阵 $\boldsymbol{I}$.$\boldsymbol{J}_k$ 表示 1 个 n 维离散混沌系统第 k 次迭代的雅可比矩阵.令 $\boldsymbol{A}_1=\boldsymbol{J}_1\boldsymbol{U}_0=\boldsymbol{J}_1\boldsymbol{I}$,基于 SVD 可得 $\boldsymbol{A}_1=\boldsymbol{U}_1\boldsymbol{\Sigma}_1\boldsymbol{V}_1^{\mathrm{T}}$,其中 $\boldsymbol{\Sigma}_1=\mathrm{diag}(\sigma_1^{(1)},\sigma_2^{(1)},\cdots,\sigma_n^{(1)})$;

步骤 2　令 $\boldsymbol{A}_2=\boldsymbol{J}_2\boldsymbol{U}_1$,由 SVD 得 $\boldsymbol{A}_2=\boldsymbol{U}_2\boldsymbol{\Sigma}_2\boldsymbol{V}_2^{\mathrm{T}}$;

步骤 3　以此类推,使 $\boldsymbol{A}_k=\boldsymbol{J}_k\boldsymbol{U}_{k-1}\,(k=1,2,\cdots,L)$,其中 $\boldsymbol{A}_k$ 可通过 SVD 被分解为 $\boldsymbol{U}_k\boldsymbol{\Sigma}_k\boldsymbol{V}_k^{\mathrm{T}}$;

步骤 4　基于步骤 1~3,L 个对角矩阵 $\boldsymbol{\Sigma}_k$ 能被表示为

$$\boldsymbol{\Sigma}_k=\begin{bmatrix}\sigma_1^{(k)} & & & \\ & \sigma_2^{(k)} & & \\ & & \ddots & \\ & & & \sigma_n^{(k)}\end{bmatrix},\ 1\leqslant k\leqslant L. \tag{3}$$

在动力学系统中,连续迭代的雅可比矩阵连乘反映了系统相空间在演化过程中的局部拉伸与折叠行为.通过对每次迭代形成的矩阵 $\boldsymbol{A}_k=\boldsymbol{J}_k\boldsymbol{U}_{k-1}$ 进行奇异值分解,所得的奇异值 $\sigma_i^{(k)}$ 恰好代表了第 k 次迭代中,相空间在第 i 个主方向上的局部拉伸因子.根据 Lyapunov 指数的定义,它是衡量相邻轨迹在相空间中平均指数发散率的指标.经过 L 次迭代后,第 i 个方向上的总拉伸量等于各次迭代拉伸因子的累乘,即 $\prod_{k=1}^{L}\sigma_i^{(k)}$.为了求取平均指数发散率,需要对该累乘积取对数,从而将乘积转化为连加运算,并除以总迭代次数 L,再取极限 $L\to\infty$.基于上述分析,n 维离散混沌系统的 n 个 Lyapunov 指数的计算式为

$$\left.\begin{aligned}\mathrm{LE}_1&=\lim_{L\to\infty}\frac{1}{L}\sum_{k=1}^{L}\ln\left|\sigma_1^{(k)}\right|,\\ \mathrm{LE}_2&=\lim_{L\to\infty}\frac{1}{L}\sum_{k=1}^{L}\ln\left|\sigma_2^{(k)}\right|,\\ &\vdots\qquad\qquad\vdots\\ \mathrm{LE}_n&=\lim_{L\to\infty}\frac{1}{L}\sum_{k=1}^{L}\ln\left|\sigma_n^{(k)}\right|.\end{aligned}\right\} \tag{4}$$

1.2　无简并超混沌系统构建法

在动力学系统分析中,Lyapunov 指数(LE)用于衡量动力学系统中无限接近的轨迹之间的分离速率.LE 的数量等于系统相空间的维数.如果 1 个 n 维离散混沌系统具有 n 个正的 LE,则该系统被称为 n 维离散无简并超混沌系统(n-D discrete non-degenerate hyperchaotic system, nDDNHS).所谓"无简并"是指该系统在 n 维相空间的所有维度上均表现出指数级发散特性,即所有 n 个 LE 均严格大于零,从而在全维相空间内实现了系统复杂度的最大化.此类混沌系统具有更强的动力学特性,因此更适用于混沌密码学和保密通信领域.在本节中,nDDNHS 的一般数学模型可描述为

$$\left.\begin{aligned}x_{k+1}^1&=f_2\left(g_2\left(a_2,x_k^2\right)\right)+b_2,\\ x_{k+1}^2&=f_3\left(g_3\left(a_3,x_k^3\right)\right)+b_3,\\ &\vdots\qquad\qquad\vdots\\ x_{k+1}^n&=f_1\left(g_1\left(a_1,x_k^1\right)\right)+b_1.\end{aligned}\right\} \tag{5}$$

式中:$x_k^i\,(i\in\{1,2,\cdots,n\})$ 为 nDDNHS 的状态变量;a_i 和 b_i 为系统的控制参数,$a_i,b_i\in\mathbf{N}^+$ 且 $a_i,b_i>1$.nDDNHS 的结构框图如图 2 所示,函数 $f_i(\cdot)$ 和 $g_i(a_i,x_k^i)$ 的具体表达式如表 1 所示.

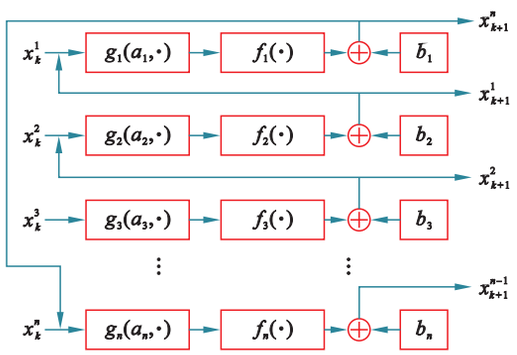


图 2　nDDNHS 的结构框图

Fig. 2　Structure block diagram of the nDDNHS

表 1　函数 $f_i(\cdot)$ 和 $g_i(a_i,x_k^i)$ 的具体表达式

Table 1　Specific expressions for the functions $f_i(\cdot)$ and $g_i(a_i,x_k^i)$

函数	Case−1	Case−2	说明
$f_i(\cdot)$	$\sin(\cdot)$	$\cos(\cdot)$	折叠操作
$g_i(a_i,x_k^i)$	$(x_k^i)^{a_i}$	$(a_i)^{x_k^i}$	拉伸操作

一般来说,混沌出现的 2 个必要条件是全局有界性和至少有 1 个正 LE.从几何角度看,混沌系统的轨迹在相空间中经历了折叠和拉伸变换.随着时间的推移,拉伸变换通过连续分离最初相邻的状态而引起轨迹发散.然而,为了防止轨迹发散到无穷大,混沌系统还需要配备 1 个折叠机制.折叠和拉伸操作会导致轨迹的指数分离和收敛,因此混沌系统对初始条件具有敏感的依赖性.这里,使用函数 $f_i(\cdot)$ 来确保 nDDNHS 是有界的,也即折叠操作.另一方面,函数 $g_i(a_i,x_k^i)$ 应用指数函数或幂函数来获得相邻轨迹的快速分离.因此,当控制参数满足一定条件时,系统有 n 个正 LE.这里本文对 nDDNHS 具有 n 个正 LE 进行相

应的证明.根据式(5),nDDNHS的雅可比矩阵可计算为

$$\boldsymbol{J}_k=\begin{bmatrix} 0 & f_2'(g_2(a_2,x_k^2))\cdot g_2'(a_2,x_k^2) & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ & & & f_n'(g_n(a_n,x_k^n))\cdot g_n'(a_n,x_k^n) \\ f_1'(g_1(a_1,x_k^1))\cdot g_1'(a_1,x_k^1) & & \cdots & 0 \end{bmatrix}. \tag{6}$$

进一步,$\boldsymbol{J}_k\boldsymbol{J}_k^{\mathrm{T}}$可表示为

$$\boldsymbol{J}_k\boldsymbol{J}_k^{\mathrm{T}}=\begin{bmatrix} (f_2'(g_2(a_2,x_k^2))\cdot g_2'(a_2,x_k^2))^2 & & & \\ & \ddots & & \\ & & (f_n'(g_n(a_n,x_k^n))\cdot g_n'(a_n,x_k^n))^2 & \\ & & & (f_1'(g_1(a_1,x_k^1))\cdot g_1'(a_1,x_k^1))^2 \end{bmatrix}=\begin{bmatrix} \lambda_k^1 & & & \\ & \ddots & & \\ & & \lambda_k^{n-1} & \\ & & & \lambda_k^n \end{bmatrix}. \tag{7}$$

显然,由于$\boldsymbol{J}_k\boldsymbol{J}_k^{\mathrm{T}}$是对角矩阵,则$\boldsymbol{J}_k\boldsymbol{J}_k^{\mathrm{T}}$的所有特征值等于$\lambda_k^i(i=1,2,\cdots,n)$且$\lambda_k^i\geqslant 0$.

定理1 假设1个$n\times n$的实数矩阵$\boldsymbol{A}$被SVD分解为$\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}}$.对角矩阵$\boldsymbol{\Sigma}=\mathrm{diag}(\sigma_1,\sigma_2,\cdots,\sigma_n)$是由$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$的所有特征值$(\lambda^1,\lambda^2,\cdots,\lambda^n)$的平方根所组成,其中$\sigma_i(i\in\{1,2,\cdots,n\})$表示矩阵$\boldsymbol{A}$的第$i$个奇异值.如果$\lambda^1\geqslant\lambda^2\geqslant\cdots\geqslant\lambda^n$,则$\sigma_i=\sqrt{\lambda^i}\ (i=1,2,\cdots,n)$.

基于LE和SVD的计算步骤,$\boldsymbol{A}_1=\boldsymbol{J}_1\boldsymbol{I}=\boldsymbol{J}_1=\boldsymbol{U}_1\boldsymbol{\Sigma}_1\boldsymbol{V}_1{}^{\mathrm{T}}$.根据定理1和式(7),$\boldsymbol{\Sigma}_1=\mathrm{diag}(\sigma_1^{(1)},\sigma_2^{(1)},\cdots,\sigma_n^{(1)})$等于$\mathrm{diag}(\mathrm{sort}(\sqrt{\lambda_1^1},\sqrt{\lambda_1^2},\cdots,\sqrt{\lambda_1^n},\text{'descend'}))$,其中$\mathrm{sort}(\cdot,\text{'descend'})$表示降序排列.接下来,由于$\boldsymbol{A}_2=\boldsymbol{J}_2\boldsymbol{U}_1=\boldsymbol{U}_2\boldsymbol{\Sigma}_2\boldsymbol{V}_2{}^{\mathrm{T}}$和$\boldsymbol{J}_2\boldsymbol{U}_1(\boldsymbol{J}_2\boldsymbol{U}_1)^{\mathrm{T}}=\boldsymbol{J}_2\boldsymbol{U}_1\boldsymbol{U}_1^{\mathrm{T}}\boldsymbol{J}_2^{\mathrm{T}}=\boldsymbol{J}_2\boldsymbol{J}_2^{\mathrm{T}}$,$\boldsymbol{\Sigma}_2=\mathrm{diag}(\sigma_1^{(2)},\sigma_2^{(2)},\cdots,\sigma_n^{(2)})$等于$\mathrm{diag}(\mathrm{sort}(\sqrt{\lambda_2^1},\sqrt{\lambda_2^2},\cdots,\sqrt{\lambda_2^n},\text{'descend'}))$.以此类推,$\boldsymbol{\Sigma}_i=\mathrm{diag}(\sigma_1^{(i)},\sigma_2^{(i)},\cdots,\sigma_n^{(i)})$等于$\mathrm{diag}(\mathrm{sort}(\sqrt{\lambda_i^1},\sqrt{\lambda_i^2},\cdots,\sqrt{\lambda_i^n},\text{'descend'}))$,$i=1,2,\cdots,L$.

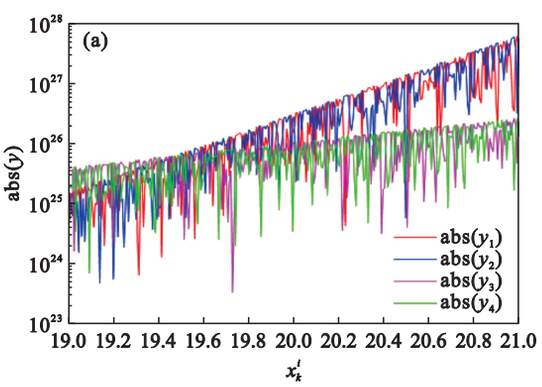
明显地,基于式(4)和式(7)可得出如下结论:如果$\mathrm{abs}(f_i'(g_i(a_i,x_k^i))\cdot g_i'(a_i,x_k^i))(i=1,2,\cdots,n)$大于1,则$n$DDNHS的所有LE皆为正.实际上,此方法可以通过控制参数a_i和b_i的值来达到上述条件.这里函数$f_i(\cdot)$和$g_i(a_i,x_k^i)$的4种组合被列在表2中.

为了便于分析,令$a_1=a_2=\cdots=a_n=a$和$b_1=b_2=\cdots=b_n=b$.基于式(5),x_k^i的取值范围可计算为$[b-1,b+1]$,也即控制参数b能够决定$x_k^i(i=1,2,\cdots,n)$的值域.本文通过固定参数$a=20$,分析了不同参数b对$\mathrm{abs}(y_i)(i=1,2,3,4)$的影响,这里abs(·)表示取绝对值运算,相应的数值仿真结果如图3所示.根据图3可知,在当前参数a和b的取值下,$\mathrm{abs}(y_i)(i=1,2,3,4)$均远大于1.此时,所有LE均大于0,因此$n$DDNHS是一个无简并超混沌系统.此外,如图3所示,当参数a和b均为稍大的正整数时,若$b\gg a$,则有$\mathrm{abs}(y_i)(i=1,2)\gg\mathrm{abs}(y_i)(i=3,4)$.反之,$\mathrm{abs}(y_i)(i=1,2)\ll\mathrm{abs}(y_i)(i=3,4)$.毫无疑问,参数$a$和$b$越大,$n$DDNHS的LE就越大.上述理论分析结果可指导此构建方法选取所需的控制参数.

表2 函数$f_i(\cdot)$和$g_i(a_i,x_k^i)$的4种组合

Table 2 Four combinations of the functions $f_i(\cdot)$ and $g_i(a_i,x_k^i)$

组合	$f_i(g_i(a_i,x_k^i))$	$f_i(g_i(a_i,x_k^i))$导数
Case−1	$\sin((a_i)^{x_k^i})$	$y_1=\cos((a_i)^{x_k^i})(a_i)^{x_k^i}\ln a$
Case−2	$\cos((a_i)^{x_k^i})$	$y_2=-\sin((a_i)^{x_k^i})(a_i)^{x_k^i}\ln a$
Case−3	$\sin((x_k^i)^{a_i})$	$y_3=\cos((x_k^i)^{a_i})a_i(x_k^i)^{a_i-1}$
Case−4	$\cos((x_k^i)^{a_i})$	$y_4=-\sin((x_k^i)^{a_i})a_i(x_k^i)^{a_i-1}$



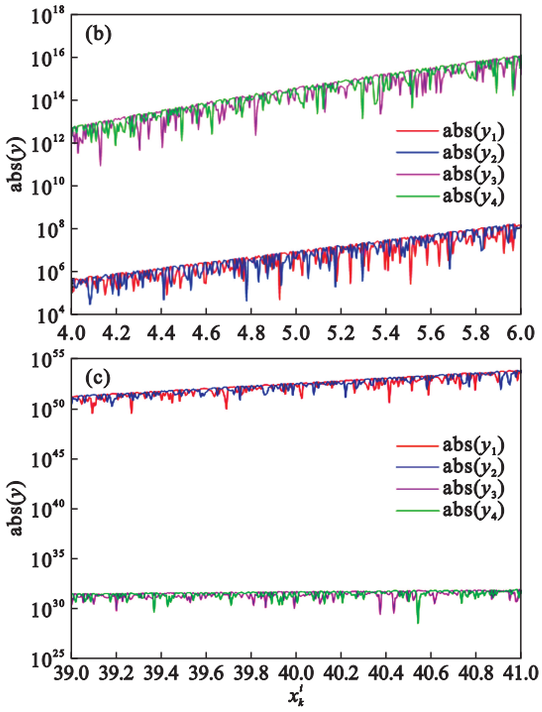


图 3　不同参数 b 对 abs(y_i)(i=1,2,3,4)的影响

Fig. 3　Influence of various parameters b on abs(y_i)(i=1,2,3,4)

(a)—b=20;(b)—b=5;(c)—b=40.

2　无简并超混沌系统构建示例

在本章中,基于上述构建方法给出 2DDNHS 和 4DDNHS 两个无简并超混沌系统示例来证明所提方案的有效性和可行性.对于 2DDNHS,本文设置 $a_2=20$,$a_1=30$ 和 $b_1=b_2=40$. 该混沌系统的数学方程可表示为

$$\left.\begin{aligned} x_{k+1}^1&=\sin(20^{x_k^2})+40,\\ x_{k+1}^2&=\cos(30^{x_k^1})+40. \end{aligned}\right\} \tag{8}$$

进一步,系统初始值设为[40.1, 40.2],2DDNHS 的 LE 被计算为 $LE_1=136.583\ 7$ 和 $LE_2=120.240\ 1$,此超混沌系统的相图如图 4 所示.

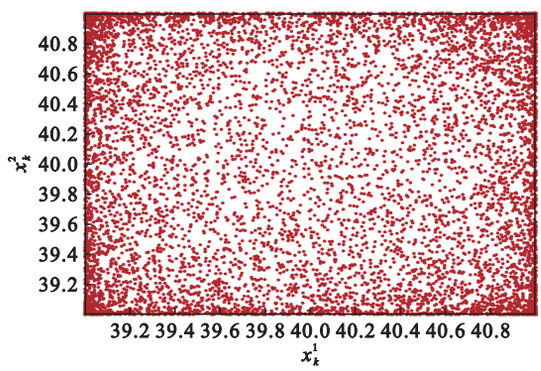


图 4　2DDNHS 相图

Fig. 4　Phase portrait of the 2DDNHS

此外,4DDNHS 的迭代方程被构建为

$$\left.\begin{aligned} x_{k+1}^1&=\sin(80^{x_k^2})+40,\\ x_{k+1}^2&=\cos(90^{x_k^3})+50,\\ x_{k+1}^3&=\sin((x_k^4)^{100})+60,\\ x_{k+1}^4&=\cos((x_k^1)^{110})+70. \end{aligned}\right\} \tag{9}$$

4DDNHS 的 LE 分别为 $LE_1=424.533\ 9$,$LE_2=406.082\ 2$,$LE_3=270.725\ 1$ 和 $LE_4=219.849\ 9$. 这里设初始值为[40.1, 50.1, 60.1, 70.1],4DDNHS 的相图如图 5 所示.从图 4 和图 5 中可以看出,这 2 个系统的相图中充满了密集的点,这表明其具有良好的遍历性.显然,基于表 2 中的 4 种组合,此构建方法可以灵活方便地构造各种维数的无简并超混沌系统.

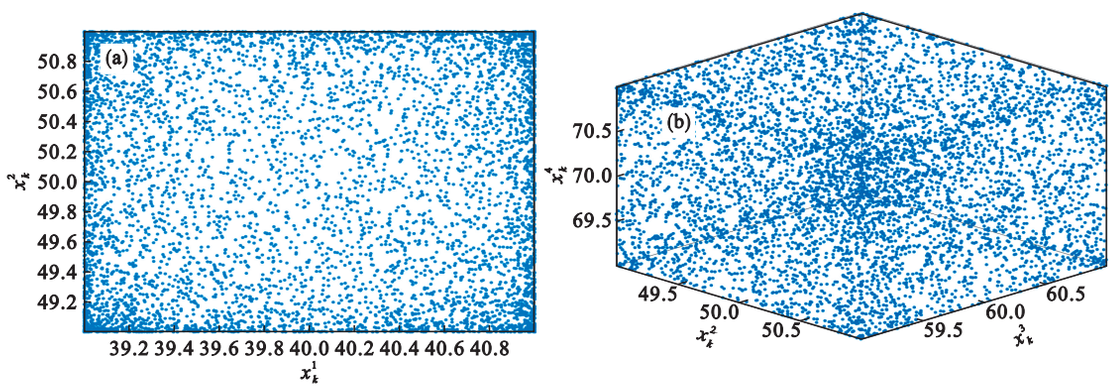


图 5　4DDNHS 相图

Fig. 5　Phase portraits of the 4DDNHS

(a)—$x_k^1-x_k^2$;(b)—$x_k^2-x_k^3-x_k^4$.

为了进一步验证本文所提的 n 维离散无简并超混沌系统(以 4DDNHS 为例)在动力学性能上的优越性,本文选取了 3 个具有代表性的模运算混沌系统进行最大李雅普诺夫指数(largest Lyapunov exponent, LLE)与谱熵(spectral entropy, SE)的横向对比.其中,3 个 4D 系统的初始值均为[0.1,

0.2,0.3,0.4],1个8D系统的初始值为[0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8],对比结果如表3所示.从表中可见,本文提出的4DDNHS系统的LLE达到424.533 9,远高于其他对比系统,表明其轨道分离速率极快,对初始条件具有极高的敏感性.此外,4个系统的SE均在0.954 0附近,表明它们产生的伪随机序列在频域上均具有接近理想白噪声的均匀功率谱分布,复杂度相当.

表3 不同混沌系统的LLE与SE对比分析

Table 3 Comparative analysis of LLE and SE for various chaotic systems

混沌系统	SE	LLE
文献[16]8D	0.953 9	4.500 0
文献[19]4D	0.953 9	4.930 4
文献[20]4D	0.953 8	6.396 9
本文4DDNHS	0.954 5	424.533 9

3 PRNG构建与混沌系统DSP实现

3.1 基于无简并超混沌的PRNG

混沌系统的良好动力学特性非常适合构建伪随机数生成器(pseudo random number generator,PRNG).在本节中,基于所提的n维离散无简并超混沌系统(nDDNHS)构造了1种简洁的PRNG,旨在应用于混沌密码学与保密通信领域.假设该混沌系统在各维度上的取值范围均为$[c_1,c_2]$.在此基础上,采用1种简洁的阈值量化方法将离散的混沌实值序列$\{x_k^i\}$转换为混沌二元序列$\{b_k\}$.该阈值量化方法的数学表达式可被定义为

$$b_k=\begin{cases}1, & x_k^i\geqslant t_{\mathrm{d}};\\ 0, & x_k^i<t_{\mathrm{d}}.\end{cases}\tag{10}$$

其中,$t_{\mathrm{d}}=(c_1+c_2)/2$为判断阈值,即取值区间的中点.

基于上述理论,本文以4维离散无简并超混沌系统(4DDNHS)为例,构造了1个混沌PRNG.为评估该PRNG输出序列的随机性,采用了NIST SP800-22统计测试套件.该测试标准由美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)制定,包含近似熵、重叠模板测试、块频数测试等15项检测指标[21].这些子测试能够有效检测二元序列在统计特性上与真随机序列之间的偏差.在本节中,基于4DDNHS以及利用所提出的PRNG生成了1个长度为10^8的混沌二元序列$\{b_k\}$.随后,将该序列划分为100个长度为10^6的子序列,并分别进行NIST SP800-22测试,测试结果如表4所示.从表中可以看出,每项统计测试的通过率均落在置信区间[0.96,1.00]内.这表明所生成的伪随机二元序列具有良好的随机性与复杂度,适合应用于保密通信等安全场景.

表4 PRNG的NIST SP800-22测试

Table 4 NIST SP800-22 test of the PRNG

测试项	$P-\mathrm{value}_{\mathrm{T}}$	通过率
频数	0.030 806	1.00
块内频数	0.637 119	1.00
累加和(前向)	0.816 537	1.00
累加和(后向)	0.867 692	1.00
游程	0.554 420	0.98
块内最长连续1游程	0.883 171	0.99
二元矩阵秩	0.236 810	0.99
离散傅里叶变换	0.779 188	0.99
非重叠模板匹配	0.224 821	0.99
重叠模板匹配	0.514 124	0.99
通用统计测试	0.935 716	1.00
近似熵	0.437 274	1.00
随机游走	0.484 646	0.99
随机游走变体	0.337 162	0.99
串行1	0.554 420	0.98
串行2	0.911 413	1.00
线性复杂度	0.897 763	1.00

注:P-value$_{\mathrm{T}}$是对所有被测序列的P-value集合进行卡方均匀性检验后得到的二级统计量,若P-value$_{\mathrm{T}}\geqslant$0.000 1,则认为这组P-value的分布是均匀的,即该测试项通过.P-value是单条序列在该项随机性检验中得到的概率值,取值范围[0,1].若P-value$\geqslant$0.01,则该条序列通过该项测试.

进一步,吞吐量是衡量PRNG实际应用价值的重要指标.本文在配置为Intel Core i7-8550U CPU@1.80 GHz的计算机上,采用阈值量化法将4DDNHS生成的混沌实值序列转换为二元序列,实测平均吞吐量为1.60 Mb/s.未来若将量化方案拓展为多比特截取量化法,系统的数据吞吐量将展现出显著的提升空间.

对于混沌PRNG,密钥空间的大小是决定其能否抵御暴力穷举攻击的决定性指标.对于本文的4DDNHS,密钥包括初始状态$(x_0^1,x_0^2,x_0^3,x_0^4)$和8个控制参数,在双精度浮点数表示下,每个初始状态分量可取值约10^{15}种.控制参数取大于1的正整数,若取值范围设为$[2,10^4]$,则总密钥空间大小为$(10^{15})^4\times(10^4)^8=10^{92}\approx 2^{305}$,其远大于密码学要求的$2^{128}$安全门限,足以抵御暴力穷举攻击.

此外,信息熵用于衡量序列中符号的不确定

性,是评估PRNG抵抗频率攻击能力的关键指标.本文生成了长度为 10^7 b的二元序列,计算其信息熵为0.999 9,极其接近理想值1.这表明序列中0和1的分布高度均匀,未显现出可被频率分析利用的明显统计偏置,因此能够有效抵抗频率攻击.

3.2　无简并混沌系统的DSP实现

混沌系统对初始条件具有极高的敏感性,而传统的模拟混沌电路易受环境温度、湿度等因素的干扰,导致其稳定性较差.相比之下,数字信号处理器(DSP)芯片具备低功耗、高稳定性以及强大的实时计算能力,因而在混沌安全通信领域得到了广泛应用.在本节中,基于微控制器设计了1套硬件平台,用于实现所提的 n 维离散无简并超混沌系统.该平台主要由1个DSP芯片、1个数模转换器(D/A)、1台泰克TBS-1000X数字示波器以及若干外围电路构成.这里以2DDNHS为例,采用C语言编写其数学表达式.在Code Composer Studio(CCS)开发环境下,编译后的代码通过YXDSP-XDS100V3仿真器下载至DSP芯片.随后,两路离散混沌信号经D/A模块转换为连续的模拟信号,并实时显示于示波器上.DSP实验相图如图6a所示.其中示波器屏幕中显示的是2DDNHS在 XY 模式下的实时相图,与图6b数值仿真相图相比,两者几何形态高度一致.图7展示了由泰克示波器捕获的时序波形以及经量化处理后得到的二元序列.从图7可以看出,示波器呈现的信号形态与数值仿真结果高度一致,从而验证了该硬件实现方案的正确性与可行性.

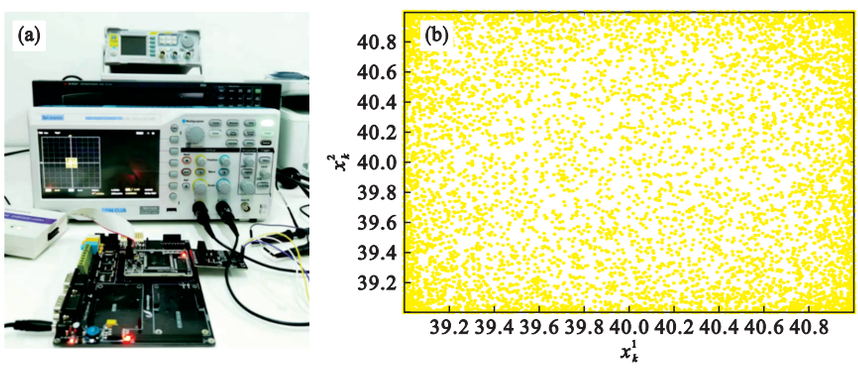


图6　2DDNHS相图对比

Fig. 6　Comparison of phase portraits for the 2DDNHS

(a)—DSP实验相图(示波器 XY 模式捕获);(b)—数值仿真相图.

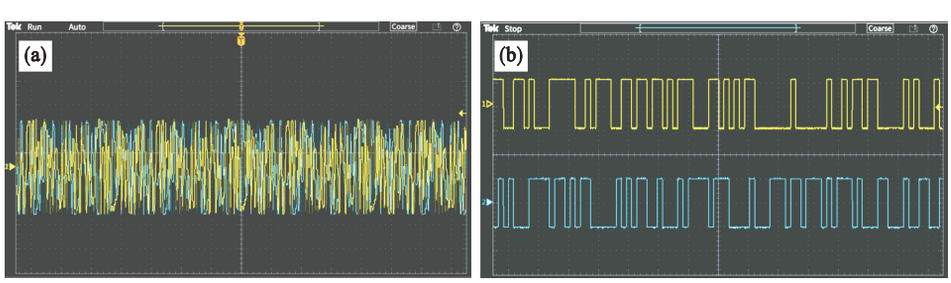


图7　示波器捕获的2DDNHS相关输出信号

Fig. 7　Relevant output signals of the 2DDNHS captured by oscilloscope

(a)—时序图;(b)—二元序列图.

4　结　　语

由于微处理器有限的计算精度,数字混沌系统的动力学特性会出现严重的退化,这限制了其在混沌密码学等领域的应用.为从根源上缓解这一问题,本文创新性地提出了1种结构简洁的 n 维离散无简并超混沌系统,该系统能够产生任意所需数量的正Lyapunov指数.具体而言,所提出的迭代模型通过引入幂函数与指数函数,实现了相邻轨迹的快速分离.这种设计不仅使系统拥有足够大的Lyapunov指数,还显著增强了对初始条件的敏感性.此外,本文通过2个典型示例(2DDNHS和4DDNHS)验证了所提方法的可行性与有效性.在应用层面,基于阈值量化方法设计了1个混沌伪随机数生成器,初步展现了所提的混沌系统的实际潜力.在未来工作中,将进一步探索复数域中混沌系统的无简并构造

方案,以拓展其在更复杂信号处理与保密通信中的应用.

参考文献:

[1] da Silva S S, Cardoso M, Nardo L, et al. A new chaos-based PRNG hardware architecture using the HUB fixed-point format[J]. *IEEE Transactions on Instrumentation and Measurement*, 2023, 72: 2001208.

[2] Li S L, Liu Y Z, Ren F Y, et al. Design of a high throughput pseudorandom number generator based on discrete hyper-chaotic system [J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2023, 70(2): 806−810.

[3] Akgul A, Kacar S, Aricioglu B. A new two-level data hiding algorithm for high security based on a nonlinear system[J]. *Nonlinear Dynamics*, 2017, 90(2): 1123−1140.

[4] Liu J Y, Zhang J G, Wang Y C. Secure communication via chaotic synchronization based on reservoir computing[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2024, 35(1): 285−299.

[5] Sharma N, Kumar P, Rai S K. Chua's oscillator-based RSA algorithm with authenticated masked public key for secure communication[J]. *IEEE Transactions on Consumer Electronics*, 2023, 69(4): 1124−1132.

[6] Fan C L, Ding Q, Tse C K. Counteracting the dynamical degradation of digital chaos by applying stochastic jump of chaotic orbits[J]. *International Journal of Bifurcation and Chaos*, 2019, 29(8): 1930023.

[7] Nardo L G, Nepomuceno E G, Arias-Garcia J, et al. Image encryption using finite-precision error [J]. *Chaos, Solitons & Fractals*, 2019, 123: 69−78.

[8] Liu L F, Xiang H Y, Li X J. A novel perturbation method to reduce the dynamical degradation of digital chaotic maps [J]. *Nonlinear Dynamics*, 2021, 103(1): 1099−1115.

[9] Zheng J, Hu H P. Bit cyclic shift method to reinforce digital chaotic maps and its application in pseudorandom number generator [J]. *Applied Mathematics and Computation*, 2022, 420: 126788.

[10] Liu L F, Hu H P, Deng Y S. An analogue-digital mixed method for solving the dynamical degradation of digital chaotic systems[J]. *IMA Journal of Mathematical Control and Information*, 2015, 32(4): 703−716.

[11] Hu G S. Generating hyperchaotic attractors with three positive Lyapunov exponents via state feedback control[J]. *International Journal of Bifurcation and Chaos*, 2009, 19(2): 651−660.

[12] Wang M J, An M Y, Zhang X N, et al. Feedback control-based parallel memristor-coupled sine map and its hardware implementation [J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2023, 70(11): 4251−4255.

[13] 禹思敏, 吕金虎, 李澄清. 混沌密码及其在多媒体保密通信中应用的进展[J]. 电子与信息学报, 2016, 38(3): 735−752.
(Yu Si-min, Lyu Jin-hu, Li Cheng-qing. Some progresses of chaotic cipher and its applications in multimedia secure communications[J]. *Journal of Electronics & Information Technology*, 2016, 38(3): 735−752.)

[14] He J B, Yu S M, Lyu J H. Constructing higher-dimensional nondegenerate hyperchaotic systems with multiple controllers [J]. *International Journal of Bifurcation and Chaos*, 2017, 27(9): 1750146.

[15] Huang L L, Liu J, Xiang J H, et al. A construction method of *N*−dimensional non-degenerate discrete memristive hyperchaotic map [J]. *Chaos, Solitons & Fractals*, 2022, 160: 112248.

[16] Wang C F, Fan C L, Ding Q. Constructing discrete chaotic systems with positive Lyapunov exponents[J]. *International Journal of Bifurcation and Chaos*, 2018, 28(7): 1850084.

[17] Zhang Y X, Hua Z Y, Bao H, et al. Generation of *n*−dimensional hyperchaotic maps using gershgorin-type theorem and its application [J]. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023, 53(10): 6516−6529.

[18] Fan C L, Ding Q, Tse C K. Designing *N*−D non-degenerate hyperchaotic systems via a simple circulant matrix[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2024, 71(1): 460−464.

[19] Zhang Y X, Hua Z Y, Bao H, et al. An *n*−dimensional chaotic system generation method using parametric Pascal matrix [J]. *IEEE Transactions on Industrial Informatics*, 2022, 18(12): 8434−8444.

[20] Fan C L, Ding Q. Design and geometric control of polynomial chaotic maps with any desired positive Lyapunov exponents [J]. *Chaos, Solitons & Fractals*, 2023, 169: 113258.

[21] National Institute of Standards and Technology. A statistical test suite for random and pseudorandom number generators for cryptographic applications: NIST SP 800−22 Rev. 1a [S]. Gaithersburg: National Institute of Standards and Technology, 2010.